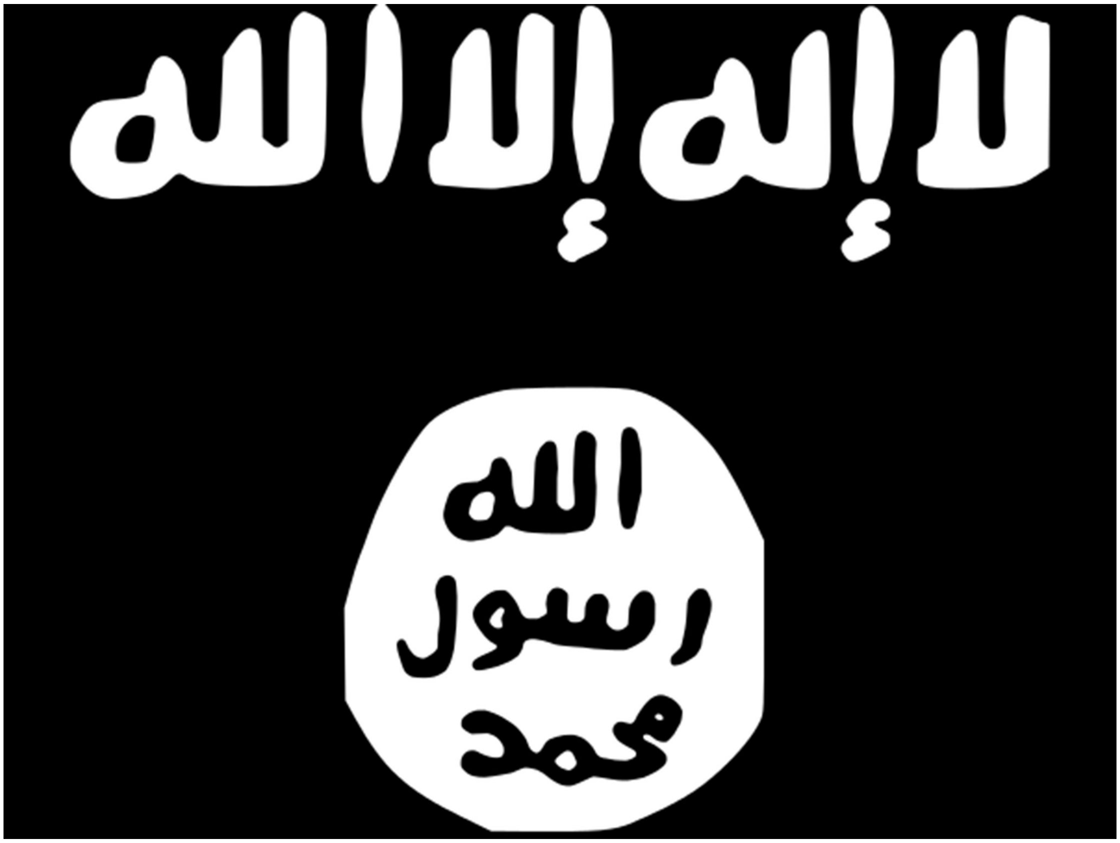
TWS
The Wilberforce Society



Terrorism of the Islamic State: Social Media Strategies

Writers: Qu Tianlu, Chia Jeng Yang, Beatrice Chan,
Chiu Chai Hao

Formatted By: Brendan Tan

The Wilberforce Society
Cambridge, UK

www.thewilberforcesociety.co.uk
February 2016

Contents

Introduction

Since its most recent emergence under the leadership of Abu Bakr al-Baghdadi in 2014, the Islamic State (IS) has been highly visible and active across various global social media platforms - those very platforms over which we engage family, friends and colleagues in our daily routine. Through footages of hostage beheadings and videos of heroic exploits, IS is sending out a powerful message reminding us of their existence, who they are and what they want. However, of even greater concern, it has launched a highly successful social media recruitment campaign. Westerners, with no ties to the Middle East whatsoever, are heading to Syria on an unprecedented scale to participate in their conflict, fighting on the side of IS.

A report by the UN Security Council in October 2014 finds that 15,000 people have travelled to the Middle East to fight alongside IS and similar extremist groups. This encompassed thousands of citizens of Western European countries, including more than 500 Britons. They have joined the militant state and almost all have taken part in their operations. These recruits are mainly teenagers and most are not even Muslims. There is substantial evidence that they were enticed by what IS had to offer through social media propaganda. IS presence on social media is not trivial; it is defined by high quality video productions and intensive following over familiar channels such as Facebook, Twitter, Instagram and YouTube. These IS productions glorify the life of an Islamic warrior (or the wife of one), and convince the public to abandon their apparent meaningless Western lifestyles for a purposeful way of life. Fighters from Western countries who were already recruited had been known to reach out to their friends and relatives back home to urge them to join. It is without a doubt that social media platforms have become the virtual recruitment centres for IS in Western countries.

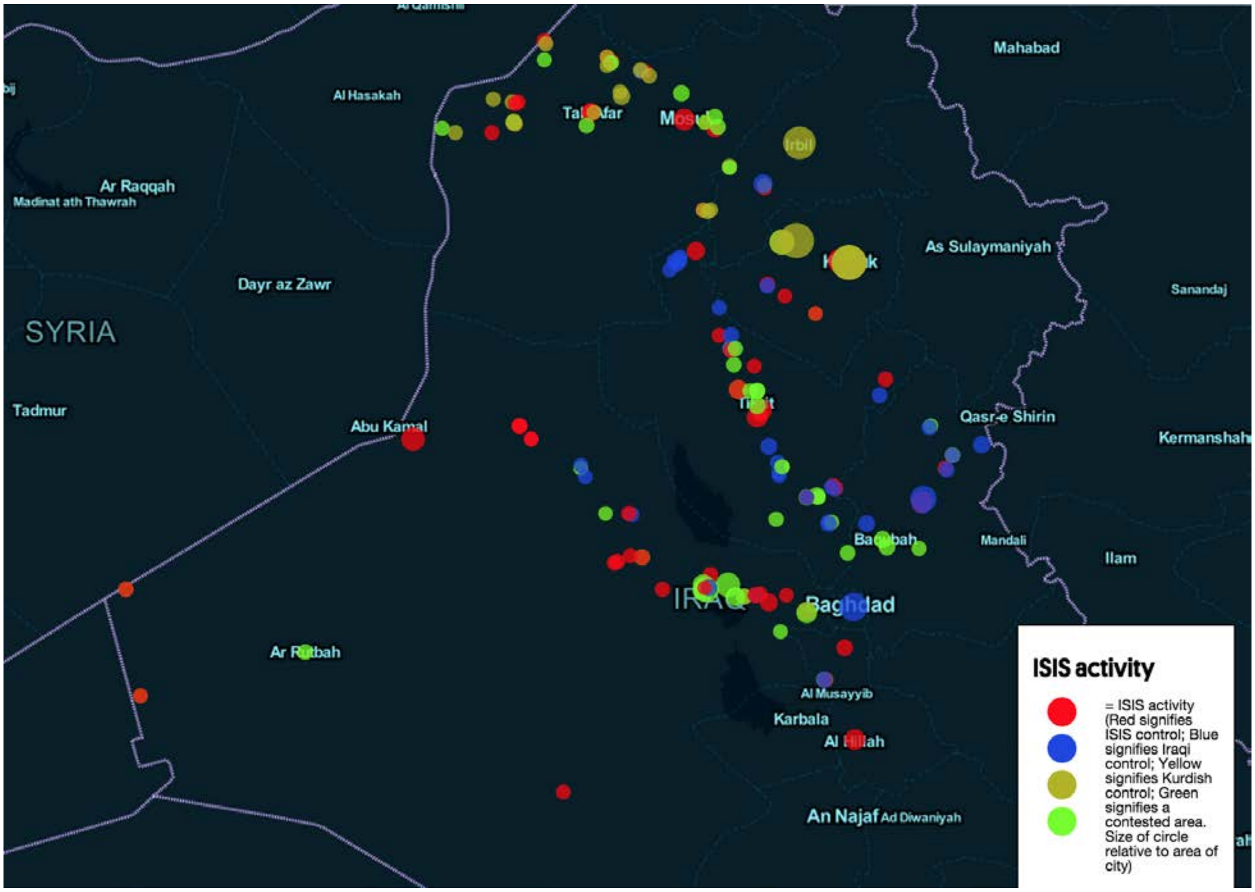
In this paper, we will examine briefly the background of Islamic State and its manifestation over various social media platforms. We will study how IS capitalised on the advantages conferred by each type of platform to achieve its ends. Subsequently, we will look at social reactions against these activities over social media. Most importantly, we would like to highlight the lack of coordinated UK governmental presence with social media providers to address the problem of IS. This is largely attributed to a confused relationship between the government and social media companies, which will be explored. In the last but most important part of the paper, we will offer our recommendations for a possible framework in which governmental bodies and social media companies could cooperate with minimal compromise of privacy and security. Our strategy involves directly engaging IS over social media platforms to regain the attention of youths in the short-run, assisting social media companies in mining and analyzing big data from their databases, followed by utilising the data to identify and respond to potential recruits. We believe that this will not only completely take apart IS' social media campaign but also construct a foundation over which the government and social media companies could work together against any future threats.

Background

Who is IS?

The Islamic State of Iraq and Syria, or ISIS in short, is also known as the Islamic State in Iraq and the Levant (ISIL), or simply the Islamic State (IS). It is a radical Islamist group and its tactics include mass killings and brutal kidnaps of ethnic and religious minorities, and international journalists. This has provoked rage and fear worldwide but its publicity of violence also entices some radical Westerners.

The aim of IS is to establish a "caliphate": a state that is ruled solely by one political or religious leader under Islamic law, or Sharia (BBC News, 2014). Their current leader is Abu Bakr al-Baghdadi, who promises to lead IS to expand past the borders of Jordan and Lebanon. As of August 2014, IS has gained control of about one third of Iraq and territories in eastern Syria within a short span of three years. IS comprises a resurgence of the Islamic State of Iraq that attempted to control Western Iraq in 2003-2006, and is sponsored by al-Qaeda, and Sunni Syrian rebel groups including the al-Nusra Front that has ties to al-Qaeda (Bryen and Johnson, 2014).



Spread of IS control, as of Jan 2015 (Security Data, 2015)

IS originated from the late Abu Musab al-Zarqawi, a Jordanian linked to the founding of Tawhid wa al-Jihad in 2002. Zarqawi pledged allegiance to Osama Bin Laden a year after the United States invaded Iraq, and formed al-Qaeda in Iraq (AQI), but his tactics were deemed "too extreme" by al-Qaeda leaders. After Zarqawi's death in 2006, AQI was merged into the umbrella organisation Islamic State in Iraq (ISI) and led by Baghdadi in 2010. Although US troops had weakened ISI's military strength considerably, Baghdadi restored ISI's might after assuming leadership. By 2013, ISI was responsible for dozens of attacks in Iraq each month, and set up the al-Nusra front with Syrian rebels against President al-Assad (BBC News, 2014).

In April 2013, Baghdadi declared the merger of his Iraq and Syrian forces to create ISIL. Although this move was rejected by al-Qaeda and al-Nusra, loyal fighters of Baghdadi left al-Nusra to join IS, and continue their fight in Syria. In December 2013, IS re-focused back to Iraq and used the political confrontation between the Shia-led government and the Sunni minority to its advantage to gain a hold on the central city of Falluja. In June 2014, after its Mosul invasion in addition to the numerous cities and towns IS had taken control of, it declared the creation of a caliphate, henceforth going by the name Islamic State (BBC News, 2014).

IS was initially funded by many rich and religiously connected Gulf donors. One striking example was Kuwait's former Minister of Justice and Islamic Affairs and Endowments, Nayef al-Ajmi, who was later sanctioned by the United States' government for funding Syrian jihadists. Later on, IS' vast financial supplies were obtained through raids of oil fields and processing facilities in Iraq, including control over Baiji, a major oil refinery site in Iraq. It also taxes small and large businesses in areas it has control of. Its robbery of the Mosul central bank in June 2014 that made headline news further added $429 million to the militant group's already deep pockets (Bryen and Johnson, 2014).

Old Threats, New Strategies

Use of social media for recruitment is not a new phenomenon among terrorist organizations, although the employment of social media by terrorist organizations differs starkly depending on their primary aims. Al-Qaeda has been using social media platforms for more than a decade to reach out to Muslim brethrens globally to join its holy war. The IS social media campaign is derived from its predecessor's, as many of their members were previously from Al-Qaeda.

Al-Qaeda has used Facebook, YouTube and various jihadist forums to spread propaganda and communicate with potential recruits. Various virtually-recruited individuals in the UK had been arrested and they were discovered making bombs using instructions found online (Briggs, 2012). Hamas and the Israeli government have repeatedly clashed over various social media platforms such as Twitter, YouTube and Facebook to denounce each other and delegitimise each other's actions (Sherwood, 2014). Various terrorist organisations also use Facebook to gather intelligence on Western military forces and privately target individual soldiers. (Weimann, 2011).

However, IS plays an entirely new game altogether. While other terror cells employ social media to complement their operations and make the occasional public announcement, IS incorporates social media as part of its strategic operations. Locally, IS might be the despotic, medieval theocracy that terrorises the populace but globally, IS is defined by its avid presence on social media. They have managed to engage audiences across the world in a way no other organizations have ever had. IS seeks global legitimacy instead of simple recognition of struggling against one or few enemies. As such, they are interested in not only recruiting 'lone wolf' terrorists to commit singular acts (such as during Charlie Hebdo attacks and the shooting at Canadian Parliament in 2014), but also targeting vulnerable segments of the Western population for radicalisation and recruitment (Shinkman, 2014). Decentralised users on social media platforms humanise the jihadist experience, allowing potential recruits to feel comfortable and find camaraderie online with IS members, potentially increasing their vulnerability for recruitment (Saltman and Winter, 2014).

Types of Social Media

Social Networking Platforms

Users can find others with similar interests and form groups and networks

IS aims to intimidate its non-believers, and inspire the impressionable minds with a convincing rhetoric. The option of unmonitored private chats provides interested readers quick and easy interaction with the terrorists.

Slickly produced war videos portray young foreign fighters in Iraq participating in dangerous, violent operations as heroes – an attempt to resonate with the impressionable audience.

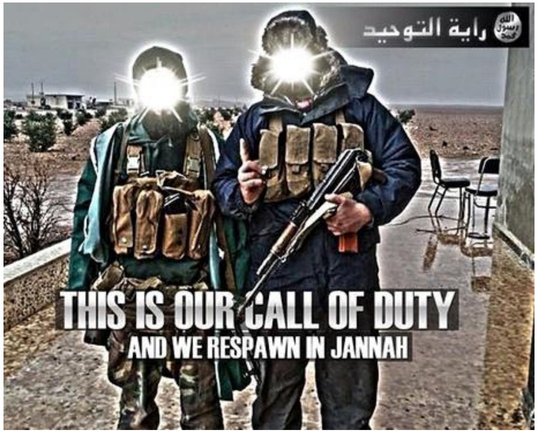
Recruiting foreign freedom fighters from the West may seem ironic, but they add to IS' rhetoric and public image.

With their contents on Facebook and Twitter removed and accounts deleted, IS recruiters gradually moved into VKontakte (VK), a Russian social media website around July 2014. A Russian technology news website, Apparat, reported extensive IS networks present over VK with recruitment content in Russian and Arabic (Global Voices, 2014). Although VK had begun removing IS related content, especially after the feature by Apparat, this proliferation shows us that our attention cannot be simply placed on familiar western social media platforms (Franceschi-Bicchierai, 2014).

Examples

Facebook, LinkedIn, VKontakte

The picture below demonstrates IS' awareness of popular culture of the West and their intent to appeal to the target audience (Smart, 2014).



Another image taken from ISIS Facebook:

Microblogging

Users can subscribe to other users' content and share related subject rapidly using hashtags.

Twitter is IS' most commonly used social media

Twitter, Tumblr

platform, followed by Facebook and YouTube. In addition to spreading radical content, IS also uses Twitter as a psychological weapon to confront and intimidate Westerners by projecting the image that they reside in various Western countries.

They ride on wholly unrelated but trending topics and hashtags to attract attention. These include the World Cup and the Scotland referendum for independence, #FIFA2014 and #IndependentScotland.

Twitter has also become a tool for IS to show both the outside world and the locals its ability to govern areas under its control. The images of IS to the locals show fighters passing out candies, with piles of corpses in the background.

A Jordanian pilot, First Lt. Moaz al-Kasasbeh, was captured by IS after his fighter jet was shot down. There was Twitter discussion over how the captors should execute him and eventually decided on burning him alive to simulate being killed in an airstrike (Griffin, 2014). He was later burnt to death and subsequent videos were distributed over Twitter (Gardham and Hall, 2015).

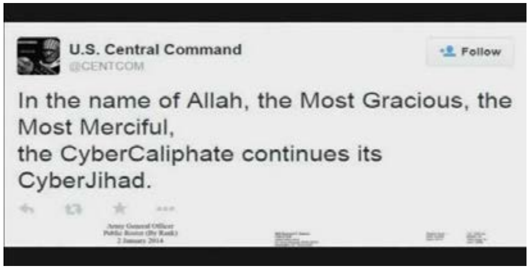
Blogging

User can share opinions, stories and articles on a personal website

Blogs are primarily used by IS for fund-raising and dissemination of general information, likely due to the less interactive nature of this platform where flow of information is largely unidirectional and passive.

Al-Khilafah Aridat: The Caliphate Has Returned, a pro-IS blog, discusses cyber-centric issues such as remaining anonymous online and how Bitcoins can be used to fund the caliphate. The anonymity and untraceability of Bitcoins allows it to be used for criminal activities and money-laundering.

More recently (Jan 12, 2015) IS followers hacked into the U.S. Central Command Twitter and Youtube accounts, posting threats and messages praising Allah.

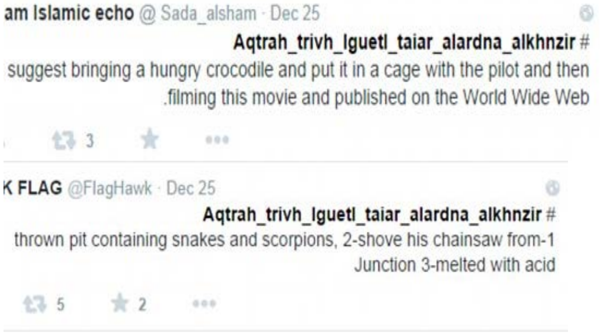


U.S. Central Command
@CENTCOM
Follow

In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate continues its CyberJihad.

Army General Officer
Public Roster (By Rank)
2 January 2014

Suggestions gathered on Twitter on how to kill the captured Jordanian pilot.

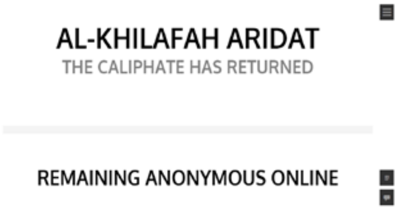


am Islamic echo @Sada_alsham · Dec 25
Aqtrah_trivh_lguetl_taiar_alardna_alkhnzir#
suggest bringing a hungry crocodile and put it in a cage with the pilot and then .filming this movie and published on the World Wide Web
3

K FLAG @FlagHawk · Dec 25
Aqtrah_trivh_lguetl_taiar_alardna_alkhnzir#
thrown pit containing snakes and scorpions, 2-shove his chainsaw from-1 Junction 3-melted with acid
5 2

Wordpress, Blogger

Screenshot of the Wordpress blog which is still available online as of 3 Feb 2015



AL-KHILAFAH ARIDAT
THE CALIPHATE HAS RETURNED

REMAINING ANONYMOUS ONLINE

<u>Photo/Video Sharing</u>

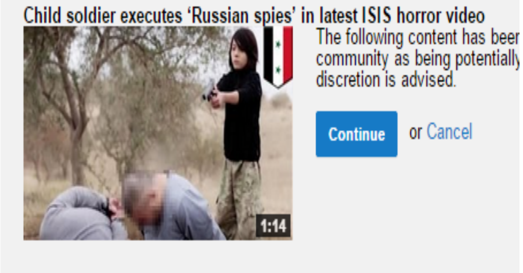
User can publish digital photos and videos and share on other social media websites.

Apart from executions of James Foley and other hostages, IS has also used videos as agents of extortion to demand money in exchange for the hostages, in the case of two Japanese men held hostage in January 2015.

Videos of the execution of one of them, Mr Goto, a journalist, were circulated on 31st January on Twitter and produced by the al-Furqan Media Foundation of IS (SITE Monitoring Service, 2015).

Instagram, Pinterest, YouTube

Screenshot from an IS video where a child soldier was shown to execute Russian spies.



Child soldier executes 'Russian spies' in latest ISIS horror video

The following content has beer community as being potentially discretion is advised.

<u>Online Forums and Chatrooms</u>

Users can use platform to raise questions and obtain instructions for various purposes.

These can be considered as the ultimate platforms of interactions as one becomes more interested in the IS ideology and wish to carry out their operations. A recent post in an IS message board included a comprehensive guide to building bombs and removing traces of their actions (Nestel et al., 2015). Radicalising and recruiting fighters are no longer the objective of forums today, likely due to the lower interactivity.

Their clandestine nature makes them elusive, only available to those who have sustained interest in it. In January 2015, Mohammed Hamzah Khan, an American youth leaving to join IS in Syria was apprehended by authorities in Chicago. He and his two siblings have followed and interacted with IS recruiters over Twitter before moving on to Kik. The latter was where the final stage of recruitment and preparations to leave for Syria took place (Sydell, 2015).

Clandestine forums, KiK, Whatsapp

Existing counter-IS activities on Social Media

Imams Online

The Imams Online website is a channel for imams, leaders of Muslim communities, worldwide to share and express their ideas with fellow Muslims. Imams in UK used this channel to broadcast a video message in July 2014 denouncing IS and urging British Muslims not to travel to war-torn regions and engage in acts of terrorism there. This is in response to an IS propaganda video featuring new British recruits who encouraged others to join. Later in the month, more than a hundred imams signed an open letter written by British Muslim leaders from leading Muslim organisations in the UK, deterring communities from joining and urging them to support those affected by IS in Iraq and Syria through aid donations.

This effort by British Muslim leaders has been recognised as the highest-profile counter-effort against the extremist group, and certainly gives credibility to the Islam religion for Muslims and non-Muslims alike (Islam Today, 2014). However, its effect is likely far less viral than IS' propaganda. Although Imams Online has a Youtube channel and Twitter account, it has few subscribers and/or followers, and its message is probably not reverberated and repeated amongst citizens. In addition, the four-minute video shows dull shots of each imam speaking against IS, a far cry from the intriguing and professionally shot videos of new IS recruits speaking of their travels from their homelands to Syria. The target audience, the segment of young Muslims who find violence appealing, are unlikely to find the imams' video compelling enough to reject IS.

Action Groups

Various action groups have come together to represent solidarity against IS. They have created a growing number of hashtags with the hopes of stopping young citizens from joining IS and educating the public about differences between Islam followers and IS extremists.

The #NotInMyName campaign is organised by an East London-based group Active Change Foundation, where young British Muslims voice their dissent against IS ideologies and stress the tagline "ISIS do not represent British Muslims" (Gadd, 2014). It went viral in September 2014, complementing the letter released in July by British Muslim leaders. Additionally in September, Inspire, a British Muslim women's group launched the campaign #MakingAStand, for Muslim women nationwide to declare their abhorrence of extremism and terrorism (Pathan, 2014). Home Secretary Theresa May was the keynote speaker at its launch and strongly supported the initiative (Home Office, 2014).

Published in October 2014 by the UK's Sun Newspaper, #UnitedAgainstIS is one of UK's latest social media campaign against IS. The Sun implored all Brits, regardless of faith, to unite against IS fanaticism, and printed the picture of a Muslim woman donning a Union Jack as her hijab on the cover page of the newspaper. Seven pages were dedicated to explaining the topic of extremism, and an additional editorial was written against Islamophobia. To support the campaign, Britians were encouraged to cut out the poster printed within a Union Jack with the caption "United Against I.S.", and upload a selfie with the poster onto a social media platform, with the #UnitedAgainstIS hashtag (Pathan, 2014).

Young men and women have gathered from across the nation to be participants of the anti-IS campaigns, and such social media campaigns indeed raise awareness. While all the campaigns should be and are applauded for their initiative, it is difficult to truly assess the extent they have prevented or changed the mindsets of radical members within the British Muslim communities.

In particular, the #UnitedAgainstIS campaign brought about polar perspectives as to whether it in fact empowers or demonises Muslim communities in the West. Several journalists of various papers applauded the Sun for its exceptional stance against IS, and its focus on establishing support for British Muslims, contrary to the Sun's previous viewpoint in various articles that were accused of slander against Muslims and being Islamophobic (Pathan, 2014). On the other hand, critics feel that this campaign and its imagery further attacks British Muslims as enemies from within who must identify their loyalty by actively participating in the #UnitedAgainstIS campaign (Malik, 2014). While a British Muslim may be inwardly horrified by IS atrocities, being pressured to showcase this distress may instead appear to be an insincere public act of conformity (Hussain, 2014). Members of the community have posted on social media sites that the article makes them feel uncomfortable as the newspaper is synonymous with Islamophobia, and a closer read hints at the lack of inclusion of Muslims within society. Furthermore, there has been relatively little social media diffusion of the campaign in comparison to IS' recruitment propaganda (Pathan, 2014). While the Sun writes to a large target audience, its message and campaign has not got widespread recognition in comparison to IS' campaign.

Governmental Actions

More than any European counterparts, the UK government has actively campaigned for greater cooperation from social media companies – most of which are US-based – to assist their efforts to combat terrorism online. Intelligence agencies believe that access to citizens' private online messages will provide valuable information to their counter-terrorism efforts. The UK government believes that the provision of private conversations of the perpetrator could have provided intelligence to prevent the Lee Rigby attack in 2013; this remains the most compelling example used by the UK government to persuade social media companies to provide relevant private information (Flynn, Fleisher and Winning, 2014). In the words of

Robert Hannigan, head of GCHQ, the UK government could allay concerns about accessing private information by 1) entering a mature public debate about privacy in a digital age, and 2) showing "how we are accountable for the data we use to protect people, just as the private sector is increasingly under pressure to show how it filters and sells its customers' data" (Hannigan, 2014). Nonetheless, Hannigan's view that privacy "has never been an absolute right" and should not hinder the greater need of anti-terror surveillance will be contentious and may be hard to gain traction – not only among the British, but also other countries at large.

The UK government has put in place various intelligence-gathering programmes. The programme Tempora operated by GCHQ and the US National Security Agency (NSA) gathers up to 30 days of internet communications data, which is mined for information on terrorist threats. The Counter-Terrorism and Security Bill was unveiled in November 2014, requiring Internet service providers to retain records on IP addresses that would help identify potential terror suspects. Counter terrorism efforts by GCHQ, MI5 and Secret Intelligence Services can be boosted by tracing IP addresses, networks and friends of the terrorist groups as they attempt to radicalise through the social media channels. However, it is increased access to private exchanges on the social media that would best facilitate counter-terrorism efforts. The debate on privacy as well as the cooperation from social media companies will be the main obstacles.

While it is important to contain and remove the radical content on social media platforms, driving terrorist communications away from mainstream social media into smaller, diffuse networks would result in the loss of critical intelligence. It may seem intuitive that the proper treatment of religious extremists on social media would be to crack down and remove such cheerleaders to prevent their voices from being heard. This is in fact the strategy employed by Twitter and Facebook (Dearden, 2014). However, there is a growing amount of evidence that suggests such actions are counter-productive. As social media platforms increase their censorship initiatives, or government's request for personal information increases, extremist and terrorist organisations simply move on to less restricted platforms, of which there are an increasing amount of alternatives. Jihadism researcher Pieter van Ostaeyen noted that 'IS supporters on social media are like mushrooms in a moist meadow – you pluck one, only for four to replace it' (Saltman and Winter, 2014). The main Jihadist discourses are now taking place on relatively more underground platforms such as Ask.fm, VK and Kik (Bland, 2014). This situation makes it harder for the government to properly monitor and counter propaganda and recruitment activities. Furthermore, it is clear that a great deal of resources would have to be devoted by the GCHQ and MI5 for the identification and removal of such voices. According to a report by the International Centre for the Study of Radicalisation (ICSR), "…the systematic, large-scale deployment of negative measures would be impractical, and even counterproductive: it would generate significant (and primarily political) costs whilst contributing little to the fight against violent extremism" (Countering Online Radicalisation A Strategy for Action, 2009).

Proposed Strategies

We propose an integrated, multi-pronged approach that includes:

(i) Drawing on the strategies from the United States counter-terrorism counterparts, to adopt the campaign of 'confront-and-correct' claims made by IS. This involves going toe-to-toe against IS on social media platforms.

(ii) Working with social media companies within clearly demarcated areas of responsibility such that privacy of citizens is minimally infringed while suspicious or malicious activity on social media platforms could be efficiently removed or responsibly monitored for valuable information. Social media companies can achieve this through utilizing big-data mining and analytics.

(iii) Using data obtained from social media platforms to profile key recruiters and content distributors. This data is promptly provided with social media companies' own discretion and used by the Home Office to identify high-risk individuals who frequent and follow these key players.

(i) Confront-and-Correct

The Internet is not the initial spark for radicalisation. Vulnerable individuals are known to be first introduced to extremist ideologies offline before being guided to extremist networks online on social media platforms. Instead of being the source of radicalisation, the Internet is a catalyst to the process, providing easy access to streams to indoctrinate, educate and socialise (Saltman and Winter, 2014). Attacking and removing extremists voices outright on certain social media platforms have been described as targeting 'a symptom rather than its cause' (Dearden, 2014). Indeed, a report by the US-based Bipartisan Policy Center, founded by politician Bob Dole found the following:

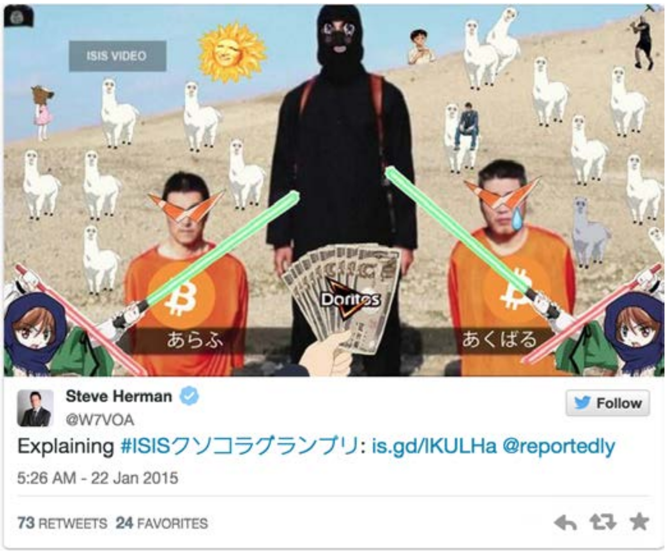
1. The filtering of Internet content is impractical in a free and open society;
2. Bringing prosecutions against propagandists often does more harm than good;
3. Relationships with Internet companies are more productive when based on partnership, not confrontation (Bipartisan Policy Center, 2012).

Such findings are in fact, very much in line with what this paper concludes. Of particular importance to the local UK context is the complicated and vague terrorism legislative environment that would make the filtering of content and prosecution of propagandists particularly problematic. In light of the Lee Rigby report, it is clear that the third point is beginning to become a contentious issue that will be of increasing importance. It is clear therefore that a confront-and-correct approach is a more desirable means of combating terrorist propaganda.

Dr. Waller, a professor from the Institute of World Politics, is a strong supporter of the use of mockery and ridicule to fight against extremist propaganda. In a series of White Papers published by the USA Today, he raises the following questions:

- Do we inadvertently aid our enemies and potential enemies by taking them too seriously?
- Does our relentless portrayal of individuals, ideologies, movements and philosophies as mortal dangers to America enhance the enemies' status and prestige?
- Is it an unsound political strategy to hype the image and power of the enemy and the few leaders who personify it?
- Is there something else the United States and its allies should be doing in their attempts to discredit, undermine and defeat the enemy (Waller, 2006)?

Dr. Waller's impactful White Paper published in 2006 was considered by the Pentagon and was largely seen as the trigger for the US mocking campaigns, which began with the publication of a video of Zarqawi wearing American sneakers and a ninja costume as he struggled to operate a US-made machine gun. It is clear that this is a campaign that the US government has continued to undertake, with the most recent campaign being a sarcastic recruitment video promoting the ethics and benefits of joining the IS (Robinson, 2014). Other governments have followed suit with such campaigns, most notably, the Pakistani government who paraded a pair of Taliban insurgents caught in woman's clothes (Waller, 2012). By having governments supporting such mocking campaigns, one is also more likely to inspire powerful cultural movements reacting against the spectre of terrorism. We can already see the beginnings of such a movement through the proliferation and popularity of IS 'fail videos', especially in the aftermath of the execution of the Jordanian fighter pilot First Lt Moaz al-Kasasbeh (The Inquisitr News, 2015). A similar effect was seen in Japan with a Japanese hashtag mocking IS going viral on Twitter. The hashtag #ISISクソコラグランプリ is translated to mean "ISIS Crappy Photoshop Grand Prix", where Twitter users photoshopped anime and other popular characters instead of the victims or executor to mock the severity of the IS pictures released.



Steve Herman
@W7VOA
Explaining #ISISクソコラグランプリ: is.gd/IKULHa @reportedly
5:26 AM - 22 Jan 2015
73 RETWEETS 24 FAVORITES

Japanese Photoshop ridicule of IS

In fact, a pro-IS group tweeted back at one photoshopped picture expressing his annoyance that "this is not a joke // Only Islam can restore your dignity!!" (Alain, 2015) Whether users employ British humour or other forms of mockery in conjunction with US mocking campaign tactics, a much more satisfactory result in terms of propagandistic effect is achieved as it increases awareness amongst a much larger number of users and undermines the terrorising message sent via IS media.

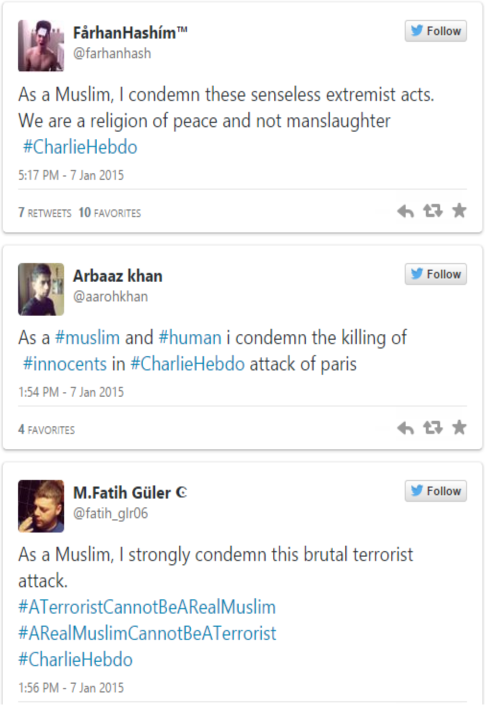
In Dr. Waller's paper, he includes an extensive history of the use of ridicule in political, cultural and armed conflicts. The advantages of using ridicule against an opponent is clear. Ridicule can help tear down one's credentials faster than one may build them. One may counter an argument, an image, or even military force, but it is difficult to defend against criticism that causes humiliation and contempt (Waller, 2006). By taking that enemy too seriously and by hyping it up as a threat, governments are unintentionally giving extremist organizations the credentials, recognition and the stature it needs to rise above its own society, establish itself, attract recruits, and gain influence (Waller, 2006). It is regarded as a principle that the more extreme the leader, the more vulnerable he tends to be to ridicule.

In January 2006, Osama Bin Laden, one of the most feared and famous terrorists in modern times, signed off a message by saying: "I swear not to die but a free man even if I taste the bitterness of death. I fear to be humiliated or betrayed." (Waller, 2006) The use of mocking campaigns strikes deeply into the psychological and ideological underpinnings of their organisations. In the case of IS, such propaganda would do well to dispel the already wavering morale of foreign fighters (Masi and FlorCruz, 2015). Such a move is supported by Peter Schweizer, a research fellow at the Hoover Institution, who affirmed the destructive effects of mockery campaigns that would engage in a psychological war 'bring[ing] these thugs down to size' (Schweizer, 2006). It is clear therefore that the UK government should do more to support and implement US-style mocking campaigns.

A significant difference between the strategies adopted by UK and the US lies in the use of 'trolls' to dispel claims of the IS, undermining their legitimacy. To fundamentally undermine the usefulness of social media to IS is to capitalise on the interactive element of the platform. This principle underlies the use of 'trolls' on social media accounts, a strategy developed in the US 5 years back. The Center for Strategic Counterterrorism Communication was formed in 2010 as the US State Department's spearhead in this "Contest of the Space". To counter messaging from Al Qaeda and its affiliated groups, the inter-agency unit engages in online forums in Arabic, Urdu, Punjabi, Somali and recently English, making itself more transparent and open to scrutiny. As the Department of State continues its foray into what some dub 'digital diplomacy', its Twitter accounts have garnered more than two million followers worldwide by last year and its Arab-language Twitter feed more than 240,000. The account engages young people, and sometimes jihadists, on websites popular in Arab countries, publishing anti-Islamic State messages, videos, on Facebook, YouTube or Twitter, using the hashtag #ThinkAgainTurnAway. The centre seeks to undermine IS and other terror groups in Somalia and Nigeria by questioning claims made by the Islamic

State, trumpeting the militants' setbacks and underscoring the human cost of their brutality (Knowlton, 2014).

However, some 50 employees of the US State Department are pitting themselves against scores of young men that populate Internet cafes round the clock, posting content from the IS media department (Knowlton, 2014). Rallying countries – from the European Union to the Middle East to Southeast Asia – to join in their cause adds strength in numbers, languages, reach and credibility. While psychologists believe that the strategy of 'trolling' could fail to convince mindsets if people feel manipulated (Knowlton, 2014), the 'trolling' attempts by different countries add credibility to unconvinced users. Apart from state actors, individual users and religious figures could be equally, or even more potent voices against the IS. At the time of writing, the Charlie Hebdo shootings in Paris by Islamic gunmen united the enraged Muslims from various parts of the world, denouncing the atrocities committed by Al-Qaeda (which the gunmen claimed to be part of) and IS (the next most likely organisation). Using the hashtag #notinmyname, tweets, posts and videos by Muslims denounce the legitimacy of these organisations and their actions (Morrison, 2015). Recognising that the IS is fighting for their own selfish and warped cause reduces its media's ability to radicalise and recruit individuals.



FårhanHashím™
@farhanhash

As a Muslim, I condemn these senseless extremist acts. We are a religion of peace and not manslaughter #CharlieHebdo

5:17 PM - 7 Jan 2015

7 RETWEETS 10 FAVORITES

Arbaaz khan
@aarohkhan

As a #muslim and #human i condemn the killing of #innocents in #CharlieHebdo attack of paris

1:54 PM - 7 Jan 2015

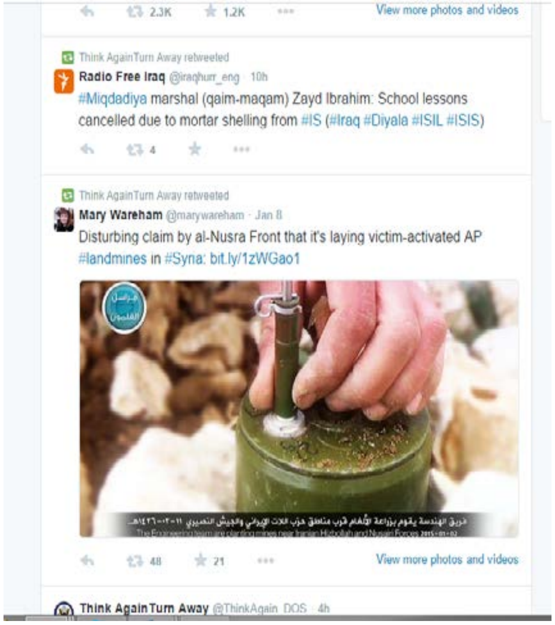
4 FAVORITES

M.Fatih Güler ©
@fatih_glr06

As a Muslim, I strongly condemn this brutal terrorist attack.
#ATerroristCannotBeARealMuslim
#ARealMuslimCannotBeATerrorist
#CharlieHebdo

1:56 PM - 7 Jan 2015

Selected screengrabs: ISIS may fight for a warped cause, but #notinmyname



2.3K 1.2K View more photos and videos

Think AgainTurn Away retweeted
Radio Free Iraq @iraqhurr_eng · 10h
#Miqdadiya marshal (qaim-maqam) Zayd Ibrahim: School lessons cancelled due to mortar shelling from #IS (#Iraq #Diyala #ISIL #ISIS)

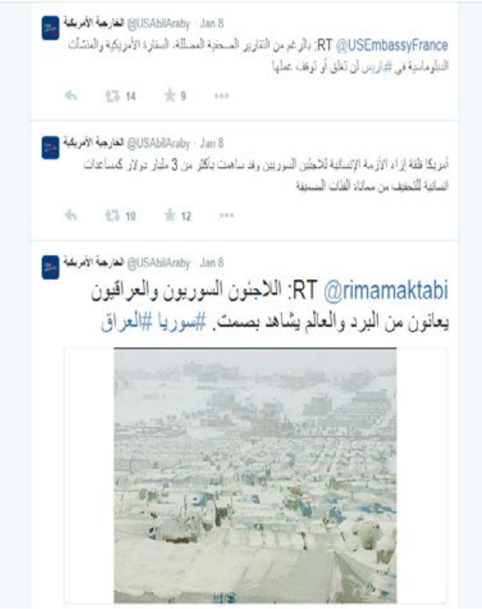
4

Think AgainTurn Away retweeted
Mary Wareham @marywareham · Jan 8
Disturbing claim by al-Nusra Front that it's laying victim-activated AP #landmines in #Syria: bit.ly/1zWGao1

فريق الهندسة يقوم بزراعة الألغام قرب مناطق حزب اللات الإيراني والجيش النصيري ١١-٠٢-١٤٣٦هـ
The Engineering team are planting mines near Iranian Hizbollah and Nusairi Forces 2015-01-02

48 21 View more photos and videos

Think AgainTurn Away @ThinkAgain_DOS · 4h



الخارجية الأمريكية @USAbilAraby · Jan 8
RT @USEmbassyFrance: بالرغم من التقارير الصحفية المضللة، السفارة الأمريكية والمنشآت الدبلوماسية في #باريس لن تغلق أو توقف عملها

14 9

الخارجية الأمريكية @USAbilAraby · Jan 8
أمريكا قلقة إزاء الأزمة الإنسانية للاجئين السوريين وقد ساهمت بأكثر من 3 مليار دولار كمساعدات انسانية للتخفيف من معاناة الفئات الضعيفة

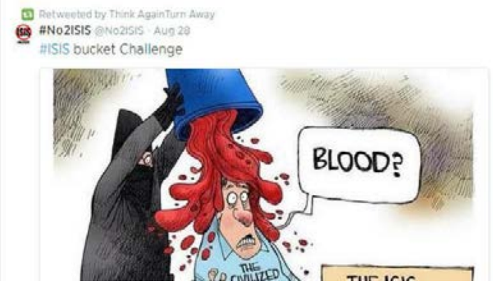
10 12

الخارجية الأمريكية @USAbilAraby · Jan 8
RT @rimamaktabi: اللاجئون السوريون والعراقيون يعانون من البرد والعالم يشاهد بصمت. #سوريا #العراق

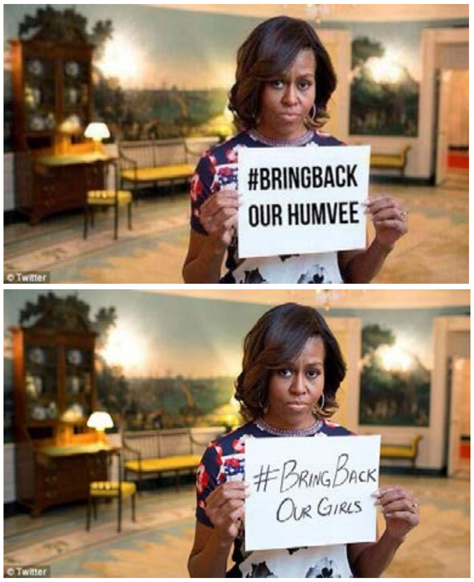
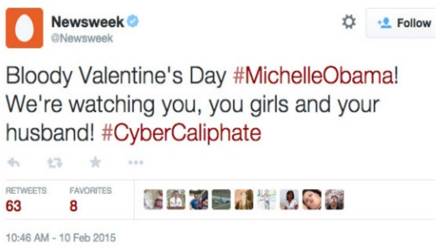
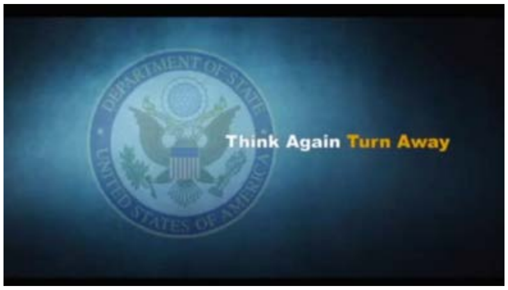
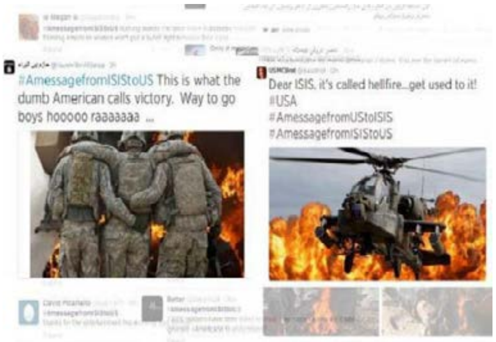
#ThinkAgainTurnAway: In English and Arabic.

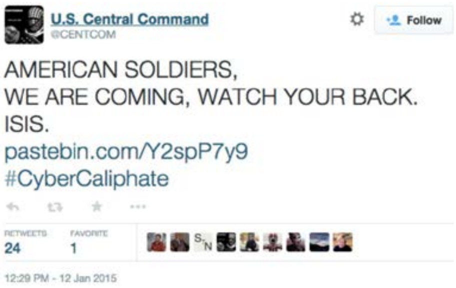
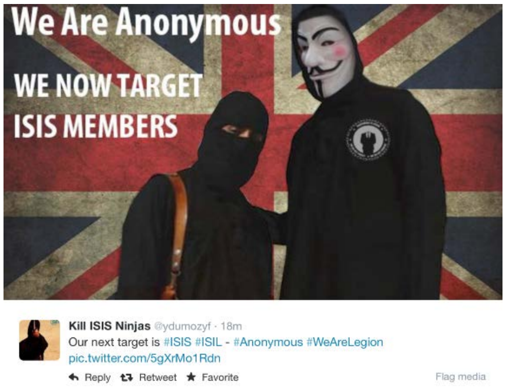
The government can rely on videos to counter IS' claims and return IS a dose of its own medicine. The videos should look professionally shot to give viewers a sense of credibility and authority, just as IS had done. They should project the tussle of emotions that fighters or recruits will face at war to depict their human side, rather than projecting them as one-sided ruthless animals, or brainwashed emotionless fanatics. This is more realistic and more likely to appeal to misguided or confused individuals toying with the idea of joining IS. The videos should be released not only on Youtube, but also websites that attract IS-inclined user traffic. Furthermore, the UK government can collaborate with private firms to produce films, television programs and various other broadcasting options to capture a wide audience. The movement should be centralised and national, and constantly talked about to be successfully embedded in citizens' minds.

Breakdown of Counter-Measures

Nature of Campaigns	**Examples of IS Strategy**	**Strategy to Counter**
Intimidation Intimidating non-believers ISIS uses social media as a psychological weapon to confront and intimidate its non-believers by projecting the image that they are capable of striking them at any point in time.	 A tweet with the hashtag #AMessageFromISIStoUS states "We are in your state. We are in your cities We are in your streets You are our goals anywhere" in front of the White House. (Martosko, 2014)	It is important to remain pre-emptive and prevent threats from becoming real attacks. This means staying vigilant and stepping up intelligence efforts. The British army will also have in place, by April 2015, Brigade 77, which consists of some 1,500 strong 'Facebook warriors' that reflects the shift towards psychological engagement on the cyberspace. (MacAskill, 2015) In countering such a psychological warfare, educating the impressionable minds (as will be discussed later) will reduce the population susceptible to ISIS propaganda.
Religious suasion and Economic enticement IS has also used social media to recruit Muslims from other countries to join their 'holy war' campaigns. They do so by: 1. Emphasising the	 Zahra Halane, 16, who made her way to Syria with her twin sister shortly after sitting her UK GCSEs. (Sherwood et al, 2014)	 Retweeted by Think AgainTurn Away #No2ISIS @No2ISIS · Aug 28 #ISIS bucket Challenge *Ice-bucket Challenge, IS-way* (Twitter) Shutting down pro-IS account and censoring objectionable content does not address the crux of the problem.

glory in the religious cause; and 2. the respectable good life that they will enjoy at the same time. IS appeals to not just young, fit males to join their cause, but also females and individuals with specialised skill sets (Khanna, 2014).	Many women have been rallied to join IS, from countries ranging from Syria, Germany, Austria to Canada. They are believed to be romanticized by the idea of war, warriors, and the opportunity to gain more respect than back home. (Bruer, 2015) Terrorism analysts at London's International Centre for the Study of Radicalisation estimate at least 30 European women in Iraq and Syria who either accompanied their jihadist husbands or have gone with the intention to marry members of ISIS and other militant groups. (Baker, 2014) Videos such as those feature Western recruits (Canadian Andre Poulin and British fighter identified as Brother Abu Bara al-Hindi) urging their compatriots to join them in a cause that they find fulfilling, meaningful and liberating – at a place where they will be taken care of. It is a balance of both gore and appeal – the former alluded to by execution videos and more recently, videos of a child soldier executing 'Russian spies'. (Shane and Hubbard, 2014)	In April 2014, IS developed an app – the Dawn of Glad Tidings – which allows IS to access their accounts to send centrally-written updates and swarm social media. As many as 40,000 tweets were posted in a single day at its peak. (McElroy, 2014) Undermining the legitimacy of the religious and moral grounds used by IS will dissuade the curious minds away from the romanticised life in IS. The same applies to non-religious campaigns too, in undermining the 'attraction' of ISIS. Such campaigns should also seek synergy from sources of authority and belief, mainly leaders of the Muslim community, for the strongest dissuasion.

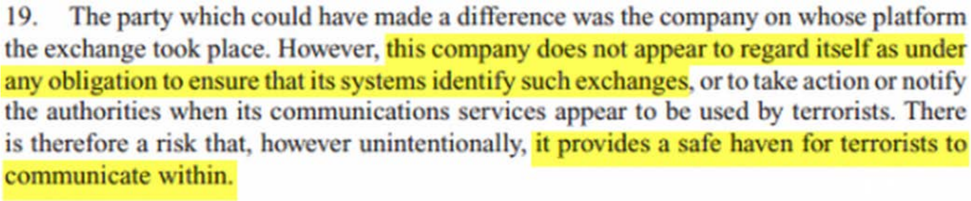
Mockery-based campaigns Used more often as a tactic to flaunt their superiority over the US incompetencies, these campaigns do not target to recruit new members, but rather to support the general IS' anti-US stance.	 #BRINGBACK OUR HUMVEE #BringBack Our Girls © Twitter © Twitter Michelle Obama's original photo in an appeal to ask the Nigerian army to #bringbackourgirls abducted by Islamic militant group Boko Haram, was photoshopped by pro-IS trolls. The doctored photo and #bringbackourhumvee tweets refer to American-made vehicles and weapons seized by IS following the retreat of the Iraqi army. (Chambers, 2014)  Newsweek @Newsweek Follow Bloody Valentine's Day #MichelleObama! We're watching you, you girls and your husband! #CyberCaliphate RETWEETS 63 FAVORITES 8 10:46 AM - 10 Feb 2015	To undermine the legitimacy and ideal scenarios that the IS promise, the US state department has started a 'Think Again Turn Away' campaign that 'confronts and contests' IS' claims, matching their slickly produced propaganda videos, 'exposing' the untruths.  DEPARTMENT OF STATE UNITED STATES OF AMERICA Think Again Turn Away This screengrab shows the slogan featured in "Welcome to the 'Islamic State' land (ISIS/ISIL)", a satirical video created by the U.S. State Department to counter English-language pro-militant propaganda. The video parodies IS recruitment by promising that followers will learn "useful new skills," such as "blowing up mosques" and "crucifying and executing Muslims."  #AmessagefromISIStoUS This is what the dumb American calls victory. Way to go boys hooooo raaaaaaa ... Dear ISIS, it's called hellfire...get used to it! #USA #AmessagefromUStoISIS #AmessagefromISIStoUS Exchanges between IS and US on Twitter illustrating US' confront and contest approach to IS propaganda. The State Department has also launched this campaign in other languages such as Arabic. (Robinson, 2014)

	 U.S. Central Command @CENTCOM AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK. ISIS. pastebin.com/Y2spP7y9 #CyberCaliphate RETWEETS 24 FAVORITE 1 12:29 PM - 12 Jan 2015 IS has also trumpeted the US incompetencies as they hack into several government accounts and posting tweets that glorify the 'CyberCaliphate' (Barnes and Yadron, 2015).	Following the killings of Jordanian pilot and Japanese hostages, 'bottom-up' cultural movements have sought to disgrace and mock IS', and could be of help to the government-led campaigns. (Bender, 2015) TV networks in the Middle East have run a satire on IS as jihadists with radical ideas and obsessed with a literal interpretation of 7th Century Islam. (Hall, 2014) ISIS VIDEO Doritos あらふ あくばる Japanese netizens mocking IS as a despotic and ridiculous organisation in their memes. (Ryall, 2015)  We Are Anonymous WE NOW TARGET ISIS MEMBERS Kill ISIS Ninjas @ydumozyf · 18m Our next target is #ISIS #ISIL - #Anonymous #WeAreLegion pic.twitter.com/5gXrMo1Rdn Reply Retweet Favorite Flag media The group of anonymous hackers are now part of IS' cyber enemies as they aim to take down IS accounts and content, paralysing their social media networks (Ou, 2015). Together with IS' attempts to hack into US government accounts on social media, a hacking arms race is being set up.

Division of Responsibility

Intensified by the revelations made by former NSA contractor Edward Snowden of mass government surveillance programs, social media platforms are making the availability and collection of data increasingly difficult. Companies prefer to remain as 'neutral conduits of data' and to 'sit outside and above politics' (Hannigan, 2014). Efforts by Google and Apple to encrypt their smartphones will hamper the intelligence agencies from accessing private data. In the Lee Rigby report, however, the UK intelligence service highlighted the lack of cooperation between government and social media companies. In his interviews and speeches in mid-January, David Cameron has pled with the largest social media companies to share responsibility in fighting the IS threat (Travis, 2014).

One of the most damning conclusions of the Lee Rigby report was the absolution of blame from UK intelligence service and the highlighting that social media companies essentially have the positive obligation to filter, detect and report any indicators from anyone who may be a terrorist element (The Intercept, 2014).



19. The party which could have made a difference was the company on whose platform the exchange took place. However, this company does not appear to regard itself as under any obligation to ensure that its systems identify such exchanges, or to take action or notify the authorities when its communications services appear to be used by terrorists. There is therefore a risk that, however unintentionally, it provides a safe haven for terrorists to communicate within.

Such a move represents an interesting expansion of the duty of care that social media companies have. Social media companies differ from traditional print media in that it facilitates content by being a service provider rather than a content provider. Such a view has been enforced by the courts in Tamiz v Google Inc [2013] EWCA Civ 68 through the common law and through regulation 19 of the 2002 European Union's electronic commerce directive [The Electronic Commerce (EC Directive) Regulations 2002]. The logical extension of such a difference would be to limit the level of liability for its content. However, we instead see the recommendation of a greater level of scrutiny for not only ordinary content but also private communications between individuals. This is akin to holding the Royal Mail liable for any malicious post sent via their services, requiring an active and total responsibility duty.

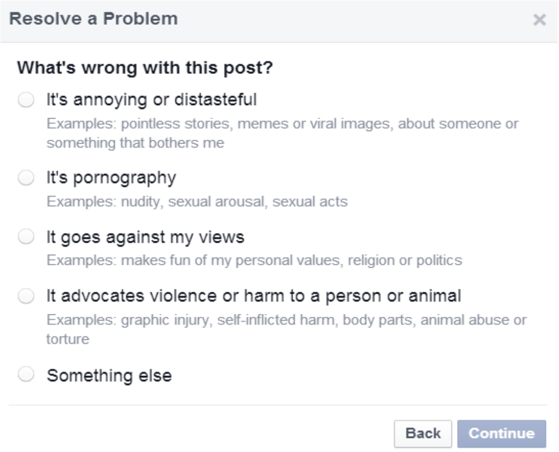
In many ways, this may not in fact be a dramatic overexpansion since we have seen similar obligations laid down onto the education system. The rights group Liberty reported that "Even our universities must read from ministers' scripts on radicalisation. Another chilling recipe for injustice and resentment by closing down the open society you seek to promote." Teaching unions expressed concern at growing pressures on the education system with the legal requirement for schools, prisons, and councils to have programmes to stop people being drawn into terrorism. The Independent revealed that one of the country's most successful schools was put into special measures for failing to monitor the activities of a sixth-form Islamic Society. Russell Hobby, the general secretary of the National Association of Head Teachers was quoted as saying that "Schools definitely have a role to play, as they protect children they also protect the neighbourhoods they serve but they are not a police service, ... a school's main contribution to the cause of anti-extremism is to provide a broad and balanced curriculum in a safe environment where human rights are respected." (The Intercept, 2014).

Perhaps it is understandable for such an attitude to arise from the government given that it would surely be much easier to sieve through internet messages than it is physical mail, and further considering the fact that most communications would be done through the internet. However, this still does not answer the fundamental and extensive breach of privacy needed ***on the part of the company*** to fulfill such a request. Internally, current content violations are handled by ordinary users flagging content that is reviewed by a team of moderators. This is as opposed to a deliberate and extensive pre-emptive privacy violating policy.

The Committee report explicitly highlighted that an examination of private messages between Michael, the perpetrator, and another was of particular significance. It is unclear how any decision to examine any such private messages by moderators can be undertaken on a non-arbitrary basis or have any real legal basis. This has not stopped current government departments such as the UK GCHQ or the USA NSA to undertake what has been widely recognized as controversial examinations of private social media communications (The Intercept, 2014).

Within the context of such a positive obligation, we see the troubling development of a general duty to monitor and police socio-political behaviours. With a simultaneous expansion of criminal liability that will be explored further later, there now exists a system with severe chilling effects.

This is, however, not to suggest that the social media companies should not be or are not resistant to all counter-terrorism efforts. While they strive to protect private exchanges, companies like Twitter and Facebook have, on multiple occasions, removed radical content from their websites or shut down accounts. Facebook claims it possesses a community standard to stop the spread of violent propaganda, and may even escalate to law enforcement (Facebook, 2015). Google (including YouTube videos) and Twitter both require human examination of reported and flagged content to remove its content (Parkinson, 2014). However, this could lead to the removed content appearing again on another account and attract greater attention (Arthur, 2014). There is a certain degree of corporate social responsibility that falls under the duty of the social media company to adopt towards the public, giving it grounds to remove content as it deems fit. As far as content regulation is concerned, IS (as well as other terrorist organisations) will continue to have its media arm entrenched in the social media, with the ease of creating a new account – an endless, online game of 'whack-a-mole' (Arthur, 2014). Government agencies and social media companies alike are frustrated over whether content should be removed or kept for further examination.


Resolve a Problem ×

What's wrong with this post?

○ It's annoying or distasteful
Examples: pointless stories, memes or viral images, about someone or something that bothers me

○ It's pornography
Examples: nudity, sexual arousal, sexual acts

○ It goes against my views
Examples: makes fun of my personal values, religion or politics

○ It advocates violence or harm to a person or animal
Examples: graphic injury, self-inflicted harm, body parts, animal abuse or torture

○ Something else

Whistleblowing on Facebook

The respective stakes and roles of the private companies and intelligence agencies in the policing of social media content should be mutually established. The element of trust should be gained from the population, both as consumers of social media and the electorate. This is done by maintaining transparency of how data will be treated, by both the companies and the government. IS recruiters and their followers adapt rapidly to escape the surveillance of the social media and agencies, and continue to proliferate on the internet; if they understand how the surveillance system work, they could create bots to fool the data mining algorithms, bringing them to banalities. To prevent this reflexivity from extremist elements, the method of surveying big data should ultimately remain classified.

Outline of Cooperation Framework between Government and Companies

	UK Government	**SM Companies**
Stakes and Interests	● Trust and support of the electorate ● National security ● Eventual elimination of IS	● Operational profits (increased costs of surveillance and big-data analytics undesirable) ● Trust and patronage of consumers
Spheres of Influence	● Policy-making ● Vast amount of manpower and resources	● Direct access to and control over relevant data ● Niche expertise
Areas of Responsibility	● Support the conduct of big-data analytics ● Provision of necessary platforms to facilitate content reporting ● Supplementary analytic work if necessary ● Acting on processed information (intelligence)	● Collection of information (Big data) ● Preservation of consumer privacy ● Analysis of big-data ● Prompt flagging of suspicious individuals and malicious content to government agency

We propose a cooperation framework between the UK government and her respective agencies with private social media companies that accounts for individual interests and intents. The detailed strategy of how big data will be collected, analysed and utilised will be discussed shortly in the next section of the paper. Social media companies, with direct access to consumer data, would conduct the preliminary "intelligence-gathering" and subsequent analysis. The government should provide the necessary expertise and financial resources if necessary to facilitate this process. At no instance, however, should the government interfere and infringe on the protected privacy of consumers either deliberately or clandestinely. The raw intelligence gathered in the form of suspicious individuals and malicious content should be referred to the government over platforms that should be established by both parties cooperatively. The agency should then decide how such information will be utilised (or removed) and could demand further updates or information based on their discretion. Social media companies should oblige to fulfill their social responsibility as much as possible within a comfortable margin. Social media companies should reserve the final say whether to release certain information.

(ii) Big Data Analytics

Big data is the term used to refer to large data sets, while data mining refers to the analytic process of studying massive data sets in search of pertinent information and consistent patterns, and then to validate the findings by applying the revealed trends or relationships on data subsets. Data mining is usually performed by data analytics or other sophisticated search operations with predictive data mining being the most common, to anticipate future behaviour and effects of change. It is done through three stages; firstly exploration which involves data transformation and selection of variables and statistical or graphical methods, secondly model building and validation to choose the best model based on its predictive performance, and finally deployment where the chosen model is applied to the data set o generate projected outcomes (Statsoft, n.d.).

Powerful data-mining tools that have been developed today are extremely efficacious in predicting "social contagions" (Woodie, 2014). One example is the Minerva Research Initiative, which was founded in 2008 and funded by the US Department of Defense in combination with the National Science Foundation (Minerva Initiative, 2014). It funds universities worldwide to conduct social science research to support US defence policy (Ahmed, 2014). One of its priority research topic areas is in 'analytical methods and metrics for security research' (Minerva Initiative, 2014). It is claimed that Minerva-funded projects successfully track the origins and growth of social movements, NGOs, extremist groups and so on, with the help of big data analytics that assess threats and analyse social media posts by tracked groups, and were able to predict the upcoming rise of IS previously (Ahmed, 2014). A common example of the use of big data is in online retail; by incorporating existing customer data, web browsing patterns, industry forecasts or trends and so forth, the retailer can optimise prices and recommend particular products to individual customers' preferences. Another example is in medical practices, where big data analytics is used to sort through a database of physical attributes, medical history and other relevant factors of a large number of individuals to successfully flag out high-risk individuals to design appropriate prevention measures for chronic diseases, including diabetes (Koh and Tan, n.d.). Potential IS recruits can be sieved out using similar data analytics, by monitoring preferred profiles accessed and followed, views and activities, which will be further described shortly. This would not differ too much in terms of scale and efficiency as compared with data mining in online retail or medical practices.

The role of big data in social media is becoming increasingly important as foreign fighters from extremist groups such as IS use social media platforms actively to document their experiences of violence and conflict that become both a source of information and inspiration. Analysing public information posted from the social media accounts of such figures can enable governments to form large amounts of insights with regards to their connections, activities, interests, and perhaps even future decisions. More importantly, finding common patterns in the social media footprints of known IS recruits could provide us with crucial information in discovering individuals who are likely to enlist. However, big data mining can be seen as a double-edged sword. While the use of big data analytics can crucially aid governments in overthrowing militant groups such as IS, there are worrying concerns associated with Pentagon-funded research initiatives such as Minerva. There are ethical and private risks associated with the government's possibly illegitimate collection of data. If the legal and social boundary is overstepped, the use of big data may backfire as it is controversially obtained and reputations of authoritative bodies are at stake (Buytendijk and Heiser, 2013). Instead, this paper suggests that social media companies should have independent power over the use of big data mining, with each individual company outlining its own structured policy in conjunction with government advice on the use of big data.

Social media companies should step in to take responsibility for media on their own platforms, and formulate their own policies that hinder extremist groups including IS from utilising the social media platforms as recruitment sources. While not explicitly removing or censoring terrorist remarks as this was proven above not to be successful, social media companies can track individuals who subscribe to known IS users who may be potential recruits. They could establish such measures in three key steps: firstly, they should establish algorithms that detect specific search keywords linked to known IS accounts or posts (key nodes). This allows the company to generate a database of users who have this area of interest. Secondly, they should monitor the specific users' accounts and posts who frequent these nodes for any signs of conversion or expressed interest to be recruited. They can also then run big data analytics on this database of users' profiles that match present IS recruits or fighters, assuming IS enlists a similar profile of militants. Finally, they should flag the high-risk individuals to the government. The government can then decide on measures to deal with these common high-risk individuals across the disparate social media platforms.

There should also be software analytics in place that function with the algorithms to run through the big data in a systematic order and create effective flags to highlight controversial topics within posts. In combination with the flagged search keywords, it allows the system to narrow down to the potential recruits to track their activities. For instance, Facebook could use their algorithm that can establish user preferences to sort out information through users' "likes", views and pages visited. For Twitter, followers of pro-IS content who condone IS acts of violence and retweet them could be tracked and profiled as high-risk individuals. If all social media companies adopt similar data mining protocol and ensure users are aware of and agree to the company's policy for privacy reasons, it should significantly assist the government in a preventive measure that is one step ahead and aware of the steps a potential recruit may take.

In fact, the hypothetical suggestions in this paper have been tested in a similar fashion and are indeed viable. A report by the International Centre for the Study of Radicalisation and Political Violence (ICSR) reveals how social media enabled them to track the population of Western fighters in Syria, and identify the spiritual authorities that Western foreign fighters look up to. To track their population, the report first defines a foreign fighter, then classifies each profile in its database as a foreign fighter or not. The profile is classified as a foreign fighter only if it fulfils two relatively strict criteria of having identified as a foreign fighter, and having documentation of himself/herself in action. Each profile is then coded to the respective affiliated organisations and nationality if listed in their social media profile information or status updates, that allowed the paper to identify the countries of origin of these foreign fighters, hence track the population of Western fighters in Syria. With regards to tracking the spiritual authorities, the report had originally created a database of social media profiles of 190 Western and European foreign fighters on Facebook and Twitter and tracked them over a year to analyse. The activity of this group revealed an uncensored window that delved straight into their minds that led to a key finding of identifying new spiritual authorities amid the Syrian conflict. These were people whom Western and European foreign fighters could look up to and relate to, and these authorities could be identified by simply analysing their social media activities (Carter et al., 2014). While the report is about militants already engaged in the conflict, this paper strives to use similar tactics to forestall members of the public from becoming radicalised into IS fighters. The fact that the findings in the report were established in such a simple, straightforward way only proves that big data analytics could be key to Western intelligence to defeat IS, especially if done on a larger scale that encompasses as many different social media platforms as possible.

(iii) Further Governmental Actions

The sheer amount of data generated by the users of internet also poses a challenge to the social media companies to mine the useful and important data. The problem of fine-tuning the algorithm to reduce the number of false positives and allow accurate identification is a common problem faced by other intelligence agencies, including the United States' NSA and its PRISM programme (Musgrave, 2013). The UK government must provide a conducive environment for social media companies to responsibly and readily conduct big-data analytics on their databases. Firstly, they need to ensure that such a policy applies to all social media companies within our definition. An unfair advantage would be conferred to companies that choose not to participate and suitable legislation should be in place to punish such an actor. Secondly, the intelligence agency must assist in the digital encryption and protection of all sensitive data obtained and transferred. Any leak will cause a lack of confidence in both the government and social media companies which will lead to the latter refusing further cooperation. Thirdly, the government must disclose this operation to the public since it concerns their privacy and will earn their trust. To withhold enough information for secrecy of operations but reveal sufficient for trust is tricky, and would come appropriately under the purview of the Privacy and Civil Liberties Board, planned to be set up to support the role of the Independent Reviewer of Terrorism Legislation (UK Government, 2014).

Certain aspects of the Counter-Terrorism and Security Bill could be encompassed into our strategy to better respond to the intelligence obtained by social media companies. In direct relation to the new powers proposed to be given to the police and Border Force officers to seize passports, high-risk individuals eligible for this treatment could potentially be expanded to those identified through data-mining. Substantial evidence collected on social media, if any, could also assist the issuance of TPIMs. The Privacy and Civil Liberties Board would further facilitate cooperation between the UK government and social media companies and maintain a healthy symbiotic relationship.

The effectiveness of our campaign against terrorism will be significantly increased with cooperation from more countries and their intelligence agencies. In a similar vein, data balkanisation threatens to hamper intelligence gathering and surveillance efforts should the internet be split into different parts as countries seek to protect their own internet data. Should it happen, discussion and coordination with the different countries to access their internet data will impede counter-terrorism efforts, including on social media. More recently, US and UK have coordinated cyber war-games to strengthen each other's cyber protection. This should be encouraged if incidents such as the US Central Command social media account hacks are to be prevented.

An educated population is a source of strength – this paper also proposes a targeted and softer approach to contest the threat of radicalisation on social media. This can be implemented on two fronts. (i) Schools and communities could educate the students and general public on ways to be a discerning consumer of social media. While there are certainly some programmes in place, in this digital age when social media is increasingly prevalent, it is appropriate to roll out a nationwide approach to equip citizens with the right skills and awareness in the marketplace of ideas. Counterterrorism education campaigns need to evolve and acknowledge the added dimension of the terrorism threat on social media platforms. Campaigns such as the National Counterterrorism Awareness Week conducted by the City of London Police, has already included some information on how one could deal with radical content on social media platforms, providing the scaffold for more cities and education institutions (City of London Police, 2015).

At the end of the day, there is a need to recognise that there is no way to completely eradicate IS influence on our social media platforms. Initially, only a small percentage of such activity could be reliably flagged out and monitored. Since our proposed strategy is not a clandestine enterprise, key IS players on various social media platforms will be more cautious regarding their footprints and find ways to mask malicious content. However, by driving IS recruiters underground, they become more obscure and cannot reach out as efficiently to radicalise new recruits. Such an outcome would not be too undesirable.

Conclusion

In this part of the paper, we have initially introduced and established the prevalent social media threat posed by IS to the Western countries including UK. The expert coordination and employment of various types of social media platforms have allowed IS recruiters to reach out broadly and deeply into our societies. There is no doubt that the IS social media campaign is well-conceived, professionally-executed and far-reaching. Existing governmental, private and societal measures to combat this campaign have been uncoordinated thus far. Our paper suggests a possible framework in which the government and social media companies could come to a compromise and collaborate. This would drastically improve the identification of individuals in high risk of joining IS and follow-up measures could be taken.

Firstly, the government should launch its own social media campaign over various social media platforms to directly enter the psychological battlefield IS has opened up. They should draw on the successes and failures of similar US strategies that have been employed over the years. Secondly, the government should, with minimal intrusion and maximum support, oblige and assist social media companies to collect and store data in their various platforms. These big data sets would then be systematically analysed to yield patterns and connections in the web of IS recruitment. Finally, the government would set up proper channels through which social media companies could submit their analysis reports. The relevant government agencies would, using their discretion, identify high-risk individuals and suspicious activities concerning IS. Such information would then be supplied to intelligence agencies to further the counter-terrorism campaign against IS.

This combination of short-term and long-term solutions seeks to dismantle the IS social media campaign and also use it against themselves. The healthy relationship promoted between government and social media companies will also be much needed to counter post-IS threats over our social networks in the increasingly interconnected world of the future.

Bibilography

Ahmed, N. (2014). *Story of a War Foretold: Why we're fighting ISIS*. [online] Ceasefire Magazine. Available at: https://ceasefiremagazine.co.uk/fighting-isis/ [Accessed 1 Feb. 2015].

Alain, S. (2015). *Twitter users in Japan mock ISIS...and it's hilarious - Viral In Nature*. [online] Viral In Nature. Available at: http://www.viralinnature.com/social-media-blog/social-media-epic-wins/item/439-twitter-users-in-japan-mock-isis-and-it-s-hilarious [Accessed 19 Mar. 2015].

Arthur, C. (2014). *Taking down Isis material from Twitter or YouTube not as clear cut as it seems*. [online] The Guardian. Available at: http://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video [Accessed 13 Feb. 2015].

Baker, A. (2014). *How ISIS Is Recruiting Women From Around the World*. [online] TIME.com. Available at: http://time.com/3276567/how-isis-is-recruiting-women-from-around-the-world/ [Accessed 13 Feb. 2015].

Barnes, J. and Yadron, D. (2015). *U.S. Probes Hacking of Military Twitter Accounts by Pro-Islamic State Group*. [online] WSJ. Available at: http://www.wsj.com/articles/u-s-investigating-apparent-hack-of-military-twitter-account-by-islamic-militants-supporters-1421086712 [Accessed 13 Feb. 2015].

BBC News, (2014). *What is Islamic State?*. [online] Available at: http://www.bbc.co.uk/news/world-middle-east-29052144 [Accessed 3 Feb. 2015].

BBC News, (2014). *'Hundreds' of UK troops to go to Iraq*. [online] Available at: http://www.bbc.com/news/uk-30464272 [Accessed 13 Feb. 2015].

Bender, J. (2015). *A Japanese Hashtag Is Mocking ISIS Amid Hostage Threats*. [online] Business Insider. Available at: http://uk.businessinsider.com/japanese-hashtag-mocking-isis-hostage-threats-2015-1 [Accessed 10 Feb. 2015].

Bipartisan Policy Center, (2012). *Countering Online Radicalization in America*. [online] Homeland Security Project. Available at: http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf [Accessed 13 Feb. 2015].

Bland, A. (2014). *Islamic State's use of social media makes joining its ranks feel easy and fun*. [online] The Independent. Available at: http://www.independent.co.uk/news/world/middle-east/islamic-states-use-of-social-media-makes-joining-its-ranks-feel-easy-and-fun-9687847.html [Accessed 5 Feb. 2015].

Briggs, R. (2012). *Discussion Paper: The Changing Face of Al Qaeda*. 1st ed. [ebook] Institute for Strategic Dialogue. Available at: http://www.strategicdialogue.org/The%20Changing%20Face%20of%20Al%20Qaeda.pdf [Accessed 1 Feb. 2015].

Bruer, P. (2015). *FBI official: ISIS is recruiting U.S. teens - CNN.com*. [online] CNN. Available at: http://edition.cnn.com/2015/02/03/politics/fbi-isis-counterterrorism-michael-steinbach/ [Accessed 13 Feb. 2015].

Bryen, S. and Johnson, M. (2014). *What is ISIS, Where did it Come From, and When Did the US Know it was There? - Jewish Policy Center*. [online] Jewish Policy Center. Available at: http://www.jewishpolicycenter.org/5376/background-what-is-isis-where-did-it-come-from-and-when-did-the-us-know-it-was-there [Accessed 3 Feb. 2015].

Buytendijk, F. and Heiser, J. (2013). *Confronting the Privacy and Ethical Risks of Big Data*. [online] Financial Times. Available at: http://www.ft.com/cms/s/105e30a4-2549-11e3-b349-00144feab7de.html [Accessed 3 Feb. 2015].

Chambers, F. (2014). *ISIS supporters mock #bringbackourgirls with #bringbackourhumvee*. [online] Mail Online. Available at: http://www.dailymail.co.uk/news/article-2661878/ISIS-supporters-make-mockery-Michelle-Obamas-campaign-bringbackourgirls-bringbackourhumvees-tweets.html#ixzz3RV8zozFT [Accessed 13 Feb. 2015].

City of London Police (2015). *National counter terrorism awareness week*. [online] Available at: https://www.cityoflondon.police.uk/news-and-appeals/campaigns-and-initiatives/counter-terrorism-awareness-week/Pages/default.aspx [Accessed 13 Feb. 2015].

Counter-Terrorism and Security Bill, Privacy Impact Assessment. (2014). 1st ed. [ebook] Gov.UK. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378941/Privacy_Impact_Assessment_MASTER_COPY.pdf [Accessed 13 Feb. 2015].

Countering Online Radicalisation A Strategy for Action. (2009). 1st ed. [ebook] International Centre for the Study of Radicalisation and Political Violence (ICSR), p.15. Available at: http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf [Accessed 5 Feb. 2015].

Dearden, L. (2014). *Islamic State: Isis fanatics threaten terrorist attacks on Twitter employees for shutting accounts down*. [online] The Independent. Available at: http://www.independent.co.uk/news/world/middle-east/islamic-state-isis-fanatics-threaten-terrorist-attacks-on-twitter-employees-for-shutting-accounts-down-9722845.html [Accessed 10 Feb. 2015].

Facebook.com, (2015). *Facebook*. [online] Available at: https://www.facebook.com/communitystandards. [Accessed 13 Feb. 2015].

Flynn, A., Fleisher, L. and Winning, N. (2014). *U.K. Steps Up Pressure on Internet Firms to Do More in Terror Fight*. [online] WSJ. Available at: http://www.wsj.com/articles/u-k-government-debuts-tougher-counterterror-laws-1417016762 [Accessed 13 Feb. 2015].

Franceschi-Bicchierai, L. (2014). *Russia's 'Facebook' Cracking Down on ISIS Accounts*. [online] Mashable. Available at: http://mashable.com/2014/09/12/isis-islamic-state-vkontakte-russia/ [Accessed 1 Feb. 2015].

Gadd, S. (2014). *Twitter campaign #NotInMyName condemns ISIS actions*. [online] The Mirror. Available at: http://www.mirror.co.uk/news/uk-news/notinmyname-young-british-muslims-stand-4274392 [Accessed 1 Jan. 2015].

Gardham, D. and Hall, J. (2015). *Was Jordanian pilot burned alive after sick ISIS Twitter campaign?*. [online] Daily Mail Online. Available at: http://www.dailymail.co.uk/news/article-2939196/Was-Jordanian-pilot-burned-alive-sick-Twitter-campaign-ISIS-supporters-method-death.html [Accessed 13 Feb. 2015].

Global Voices, (2014). *Russia Cracks Down on Internet Free Speech, Except When It's ISIS*. [online] Available at: http://globalvoicesonline.org/2014/09/11/isis-russia-social-networks-vkontakte/ [Accessed 1 Feb. 2015].

Griffin, A. (2015). [online] Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/isis-polls-twitter-for-gruesome-suggestions-of-how-to-kill-jordanian-pilot-9949550.htmlhttp://terrorismheadlines.com/2014/12/crowdsourcing-terror-isis-asks-for-ideas-on-killing-jordanian-pilot-vocativ/ [Accessed 13 Feb. 2015].

Hall, J. (2014). *Looney Tunes-style cartoon pokes fun at jihadists fighting for ISIS*. [online] Mail Online. Available at: http://www.dailymail.co.uk/news/article-2739534/ISIS-jihadis-blowing-rejecting-radio-Islamic-welcome-Iraqi-TVs-cartoon-satire-terror.html [Accessed 13 Feb. 2015].

Hannigan, R. (2014). *The web is a terroristâ€™s command-and-control network of choice - FT.com*. [online] Financial Times. Available at: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3RaX4Ard0 [Accessed 13 Feb. 2015].

Home Office, (2014). *Home Secretary supports #MakingAStand campaign - News stories - GOV.UK*. [online] Gov.uk. Available at: https://www.gov.uk/government/news/home-secretary-supports-makingastand-campaign [Accessed 1 Jan. 2015].

Hussain, D. (2014). *The Sun's 'United Against I.S.' Campaign Can't be Taken Seriously*. [online] The Huffington Post UK. Available at: http://www.huffingtonpost.co.uk/dilly-hussain/the-sun-isis_b_5956714.html [Accessed 1 Jan. 2015].

Islam Today, (2014). *Muslim Leaders across the UK Unite to Condemn ISIS*. [online] Available at: http://en.islamtoday.net/artshow-229-4878.htm [Accessed 2 Jan. 2015].

Khanna, K. (2014). *Terrorist Wanted: How ISIS Recruits Western Women | Brown Political Review*. [online] Brownpoliticalreview.org. Available at: http://www.brownpoliticalreview.org/2014/12/terrorist-wanted-how-isis-recruits-western-women/ [Accessed 13 Feb. 2015].

Knowlton, B. (2014). *Digital War Takes Shape on Websites Over ISIS*. [online] Nytimes.com. Available at: http://www.nytimes.com/2014/09/27/world/middleeast/us-vividly-rebuts-isis-propaganda-on-arab-social-media.html [Accessed 13 Feb. 2015].

Koh, H. and Tan, G. (n.d.). *Data Mining Applications In Healthcare*. 1st ed. [ebook] Journal of Healthcare Information Management - Vol. 19, No. 2. Available at: http://www.himss.org/files/himssorg/content/files/jhim/19-2/datamining.pdf [Accessed 2 Feb. 2015].

MacAskill, E. (2015). *British army creates team of Facebook warriors*. [online] the Guardian. Available at: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade [Accessed 13 Feb. 2015].

Malik, N. (2014). *The Sun's 'Unite against Isis' campaign is a proxy for anti-Muslim bigotry | Nesrine Malik*. [online] The Guardian. Available at:

http://www.theguardian.com/commentisfree/2014/oct/08/sun-unite-against-isis-muslim-bigotry [Accessed 1 Jan. 2015].

Martosko, D. (2014). *ISIS Twitter taunt includes pic of flag in front of the WHITE HOUSE*. [online] Mail Online. Available at: http://www.dailymail.co.uk/news/article-2726260/We-streets-Secret-Service-investigates-ISIS-Twitter-taunt-included-terror-groups-flag-photo-held-WHITE-HOUSE.html [Accessed 13 Feb. 2015].

Masi, A. and FlorCruz, M. (2015). *ISIS Executes Three Chinese Uighur Fighters Accused Of Defection*. [online] International Business Times. Available at: http://www.ibtimes.com/isis-executes-three-chinese-uighur-fighters-accused-defection-1806564 [Accessed 10 Feb. 2015].

McElroy, D. (2014). *Iraq crisis: Isis cracks a savvy social media advance - Telegraph*. [online] Telegraph.co.uk. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10907217/Iraq-crisis-Isis-cracks-a-savvy-social-media-advance.html [Accessed 13 Feb. 2015].

Minerva Initiative, (2014). *Priority Research Topics*. [online] Available at: http://minerva.dtic.mil/topics.html [Accessed 30 Jan. 2015].

Morrison, A. (2015). *Muslims Angered By Charlie Hebdo Attack Defend Religion In Social Media*. [online] International Business Times. Available at: http://www.ibtimes.com/muslims-angered-charlie-hebdo-attack-defend-religion-social-media-1777414 [Accessed 13 Feb. 2015].

Musgrave, S. (2013). *Does Mining Our Big Data for Terrorists Actually Make Us Any Safer?*. [online] Motherboard. Available at: http://motherboard.vice.com/blog/does-mining-our-big-data-for-terrorists-actually-make-us-any-safer [Accessed 13 Feb. 2015].

Nestel, M., Shiloach, G. and Weiss, A. (2015). *ISIS Forums Share Bomb-Making Recipe for Attacks on NYC, Las Vegas*. [online] Vocativ.com. Available at: http://www.vocativ.com/world/isis-2/isis-pipe-bomb-attack-america/ [Accessed 13 Feb. 2015].

Ou, J. (2015). *Hacking group Anonymous takes down ISIS websites, social media accounts*. [online] Straitstimes.com. Available at: http://www.straitstimes.com/news/world/middle-east/story/hacking-group-anonymous-takes-down-isis-websites-social-media-accounts- [Accessed 13 Feb. 2015].

Parkinson, H. (2014). *James Foley: How social media is fighting back against Isis propaganda*. [online] The Guardian. Available at: http://www.theguardian.com/technology/2014/aug/20/james-foley-how-social-media-is-fighting-back-against-isis-propaganda [Accessed 13 Feb. 2015].

Pathan, N. (2014). *#MakingAStand: British Muslim women launch anti-ISIS culture drive*. [online] Al Arabiya News. Available at: http://english.alarabiya.net/en/life-style/art-and-culture/2014/09/24/-MakingAStand-British-Muslim-women-launch-anti-ISIS-culture-drive.html [Accessed 1 Jan. 2015].

Pathan, N. (2014). *Does UK #UnitedAgainstIS drive, demonize or empower Muslims?*. [online] Al Arabiya News. Available at: http://english.alarabiya.net/en/life-style/art-and-culture/2014/10/14/UK-UnitedAgainstIS-campaign-launches-to-mixed-Muslim-reactions.html [Accessed 1 Jan. 2015].

Robinson, B. (2014). *US State Department slaps ISIS back with mock recruiting video*. [online] Daily Mail Online. Available at: http://www.dailymail.co.uk/news/article-2745875/War-Twitter-State-Department-releases-mock-ISIS-recruitment-film-bid-counter-terror-groups-online-pursuit-Westerners.html [Accessed 9 Feb. 2015].

Ryall, J. (2015). *Japan's social media users mock Isil with cartoons - Telegraph*. [online] Telegraph.co.uk. Available at: http://www.telegraph.co.uk/news/worldnews/islamic-state/11364390/Japans-social-media-users-mock-Isil-with-cartoons.html [Accessed 13 Feb. 2015].

Saltman, E. and Winter, C. (2014). *Islamic State: The Changing Face of Modern Jihadism*. 1st ed. [ebook] Quilliam Foundation, pp.42-43. Available at: http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/islamic-state-the-changing-face-of-modern-jihadism.pdf [Accessed 5 Feb. 2015].

Schweizer, P. (2006). *An effective weapon against terrorists: Ridicule*. [online] USA Today. Available at: http://usatoday30.usatoday.com/news/opinion/editorials/2006-03-23-ridicule-editorial_x.htm [Accessed 10 Feb. 2015].

Security Data, (2015). *How much of Iraq does ISIS control?*. [online] Available at: http://securitydata.newamerica.net/isis/analysis [Accessed 3 Feb. 2015].

Shane, S. and Hubbard, B. (2014). *ISIS Displaying a Deft Command of Varied Media*. [online] Nytimes.com. Available at: http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html [Accessed 13 Feb. 2015].

Sherwood, H., Laville, S., Willsher, K., Knight, B., French, M. and Gambino, L. (2014). *Schoolgirl jihadis: the female Islamists leaving home to join Isis fighters*. [online] the Guardian. Available at: http://www.theguardian.com/world/2014/sep/29/schoolgirl-jihadis-female-islamists-leaving-home-join-isis-iraq-syria [Accessed 13 Feb. 2015].

Sherwood, H. (2014). *Israel and Hamas clash on social media.* [online] The Guardian. Available at: http://www.theguardian.com/world/2014/jul/16/israel-hamas-clash-social-media [Accessed 1 Feb. 2015].

Shinkman, P. (2014). *Shooting at Canadian Parliament in Ottawa Raises Fears of ISIS-Prompted Attack - US News*. [online] US News & World Report. Available at: http://www.usnews.com/news/articles/2014/10/22/shooting-at-canadian-parliament-in-ottawa-raises-fears-of-isis-prompted-attack [Accessed 2 Feb. 2015].

SITE Monitoring Service, (2015). *IS Beheads Japanese Hostage Kenji Goto Jogo in Video | Jihadist News*. [online] Available at: https://news.siteintelgroup.com/Jihadist-News/is-beheads-japanese-hostage-kenji-goto-jogo-in-video.html [Accessed 2 Feb. 2015].

Smart, T. (2014). *ISIS gains followers through sophisticated social media strategy*. [online] Techgenmag.com. Available at: http://techgenmag.com/2014/10/06/isis-gains-followers-through-sophisticated-social-media-strategy/ [Accessed 25 Jan. 2015].

Statsoft, (n.d.). *What Is Data Mining, Predictive Analytics, Big Data*. [online] Available at: http://www.statsoft.com/Textbook/Data-Mining-Techniques [Accessed 30 Jan. 2015].

Sydell, L. (2015). *Pro-ISIS Messages Create Dilemma For Social Media Companies*. [online] NPR.org. Available at: http://www.npr.org/blogs/alltechconsidered/2015/01/29/382435536/pro-isis-messages-create-dilemma-for-social-media-companies [Accessed 2 Feb. 2015].

The Inquisitr News, (2015). *ISIS Fail Video Compilations Go Viral In Wake Of Jordanian Pilot's Publicized Execution*. [online] Available at: http://www.inquisitr.com/1820857/isis-fail-video-compilations-go-viral-in-wake-of-jordanian-pilots-publicized-execution/ [Accessed 7 Feb. 2015].

The Intercept, (2014). *The US/UK Campaign to Demonize Social Media Companies as Terrorist Allies - The Intercept*. [online] Available at: https://firstlook.org/theintercept/2014/11/26/campaign-shame-social-media-companies-acting-spy-agents-national-security-state/ [Accessed 13 Feb. 2015].

Travis, A. (2014). *Counter-terrorism and security bill: proposals and pitfalls*. [online] The Guardian. Available at: http://www.theguardian.com/uk-news/2014/nov/24/counter-terrorism-security-bill-proposals-pitfalls [Accessed 13 Feb. 2015].

UK Government (2014). *Counter-Terrorism and Security Bill: Privacy Impact Assessment* [online] Gov.uk. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378941/Privacy_Impact_Assessment_MASTER_COPY.pdf [Accessed 13 Feb. 2015].

Waller, D. (2006). *Los Angeles Times op-ed: US should use ridicule as weapon against its enemies - Acme of Skill*. [online] Acme of Skill. Available at: http://acmeofskill.com/2006/05/los-angeles-times-op-ed-us-should-use-ridicule-as-weapon-against-its-enemies/ [Accessed 10 Feb. 2015].

Waller, D. (2006). *Ridicule: An instrument in the war on terrorism - Acme of Skill*. [online] Acme of Skill. Available at: http://acmeofskill.com/2006/02/ridicule-an-instrument-in-the-war-on-terrorism/ [Accessed 9 Feb. 2015].

Waller, D. (2012). *Transvestite Taliban: Let's hold them up for ridicule - Acme of Skill*. [online] Acme of Skill. Available at: http://acmeofskill.com/2012/04/transvestite-taliban-us-finally-starts-holding-them-up-for-ridicule [Accessed 9 Feb. 2015].

Weimann, G. (2011). *Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking*. 1st ed. [ebook] Israeli Communication Association. Available at: http://cleanitproject.eu/files/95.211.138.23/wp-content/uploads/2012/08/2012-Terrorists-using-online-social-nerworking.pdf [Accessed 13 Feb. 2015].

Woodie, A. (2014). *How Big Data Analytics Can Help Fight ISIS*. [online] Datanami. Available at: http://www.datanami.com/2014/10/14/big-data-analytics-can-help-fight-isis/ [Accessed 31 Jan. 2015].